IBM Security Services

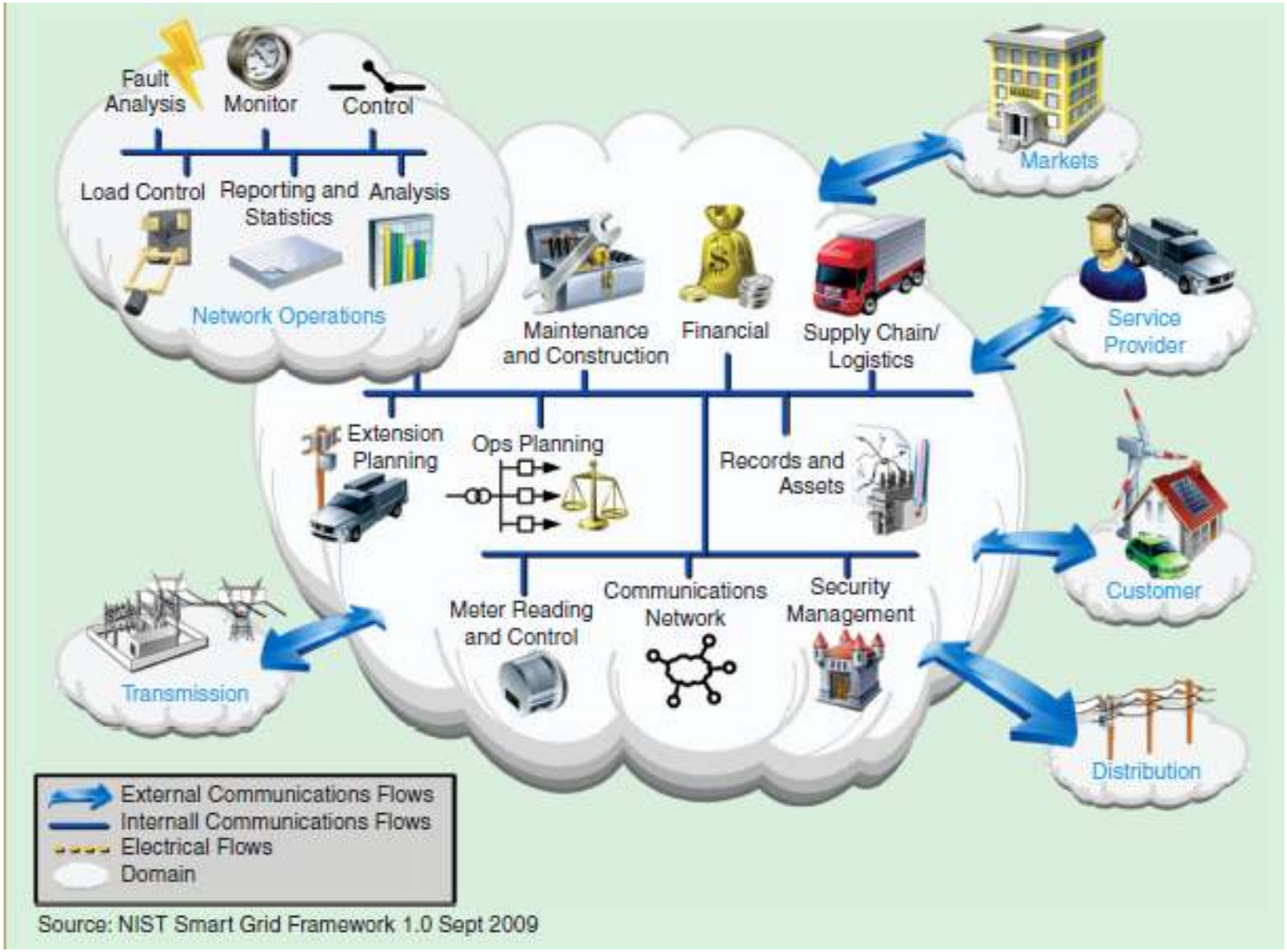
Application e SCADA Security

21 settembre 2011

Agenda

- Architetture SCADA
- Secure Engineering
- IBM Security Solutions

Operations domain from NIST interoperability framework



SCADA: tecnologie e protocolli

Field Devices

- RTU – Remote Terminal Unit
- PLC – Programmable Logic Controller
- IED – Integrated Electronic Device
- PAC – Programmable Automation Controller
- Wireless Sonsor Network (es. ZigBee)

Fieldbus Protocols

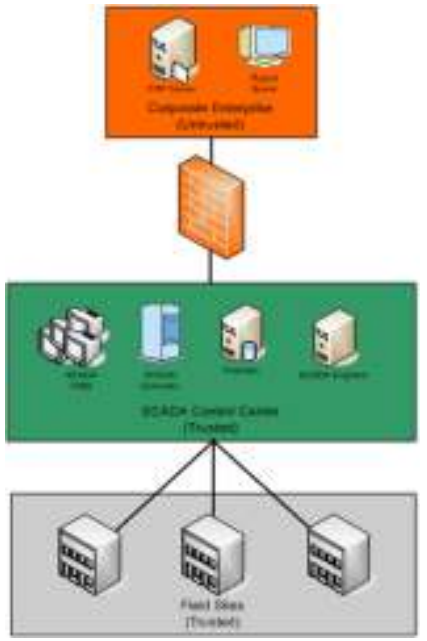
- Modbus
- DNP3
- DeviceNet

SCADA Control Center

- HMI – Human Machine Interface
- SCADA Controller – Real time processing
- Historian – database of events
- Control Center Protocols (es. OPC, ICCP)
- IIS
- Web services

Communication Technologies

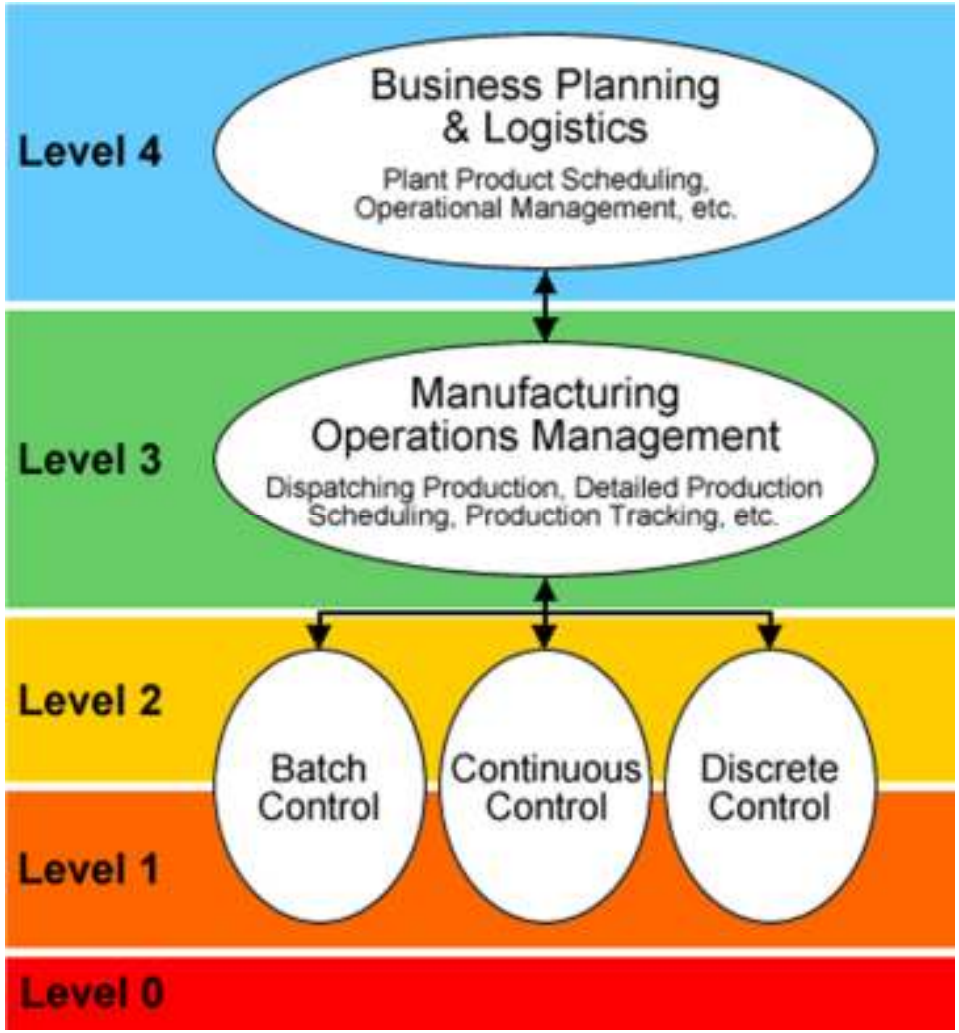
- Serial connections (hardwire & dial-up)
- Ethernet & TCP/IP / Wireless
- RF & Microwave
- Cell: CDMA



Agenda

- Architetture SCADA
- **Secure Engineering**
- IBM Security Solutions

Suddivisione ISA-95



Perchè il problema continua a crescere?

Connettività:

Internet
L'incremento del numero e delle tipologie d vettori di attacco è proporzionale all'incremento di connettività.

SOA/Web Services
Applicazioni legacy non progettate per essere in rete, sono visibili come servizi.

Sistemi Legacy
Non sempre supportano le moderne funzionalità di sicurezza (es. Autenticazione)

Estensibilità:

Il software è sempre più "estensibile" , es browser plug-in, dynamic loadable device driver

L'estensibilità dei software rende difficile prevederne la superficie di attacco nel tempo

Complessità:

La complessità delle architetture software è sempre maggiore

Nel 1990, Windows 3.1 aveva 2,500,000 linee di codice.

Windows XP ha circa 40,000,000 linee di codice.

Il numero di bugs è proporzionale al numero di linee di codice

Security Engineering & Software Development Life Cycle

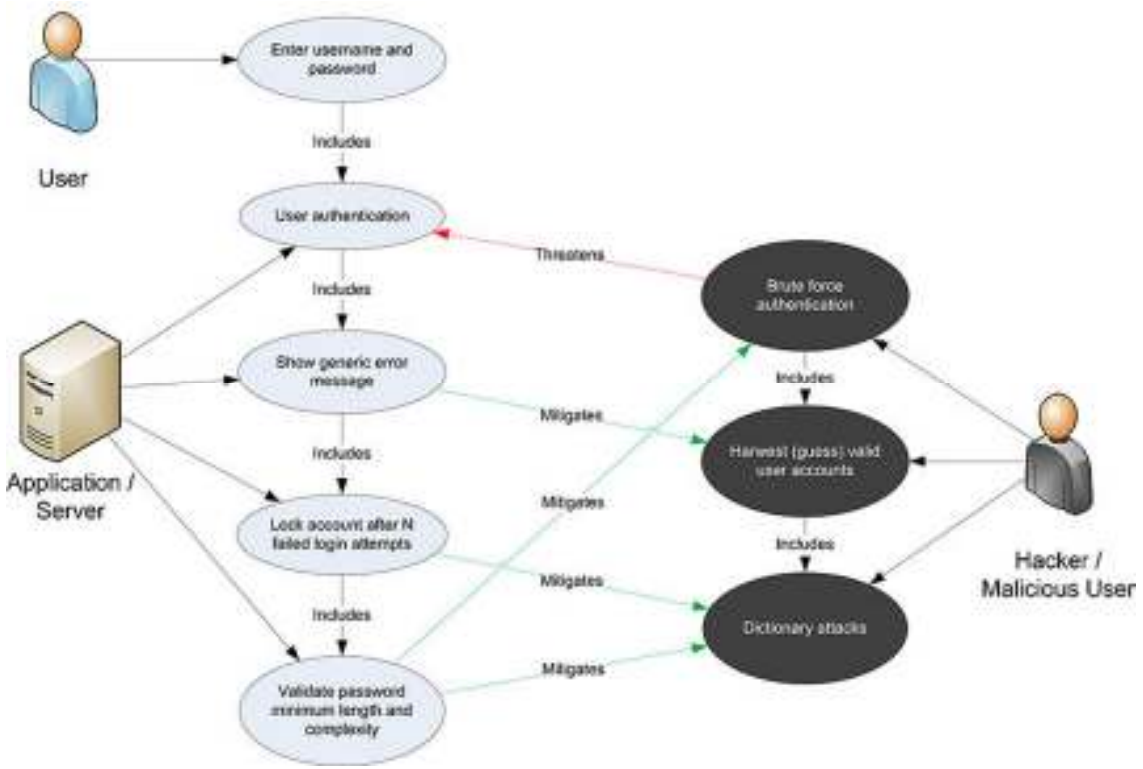
Strategia di sicurezza e metriche

Definizione dei requisiti	Design	Implementazione	Test	Deploy
Requisiti di sicurezza	Principi di secure design	Secure coding	Risk analysis	Vulnerability management
Abuse cases	Risk analysis	Revisione del codice	Security testing	Secure deployment
				Operational enablement
				Security testing

Security education

Use Cases e Misuse Cases

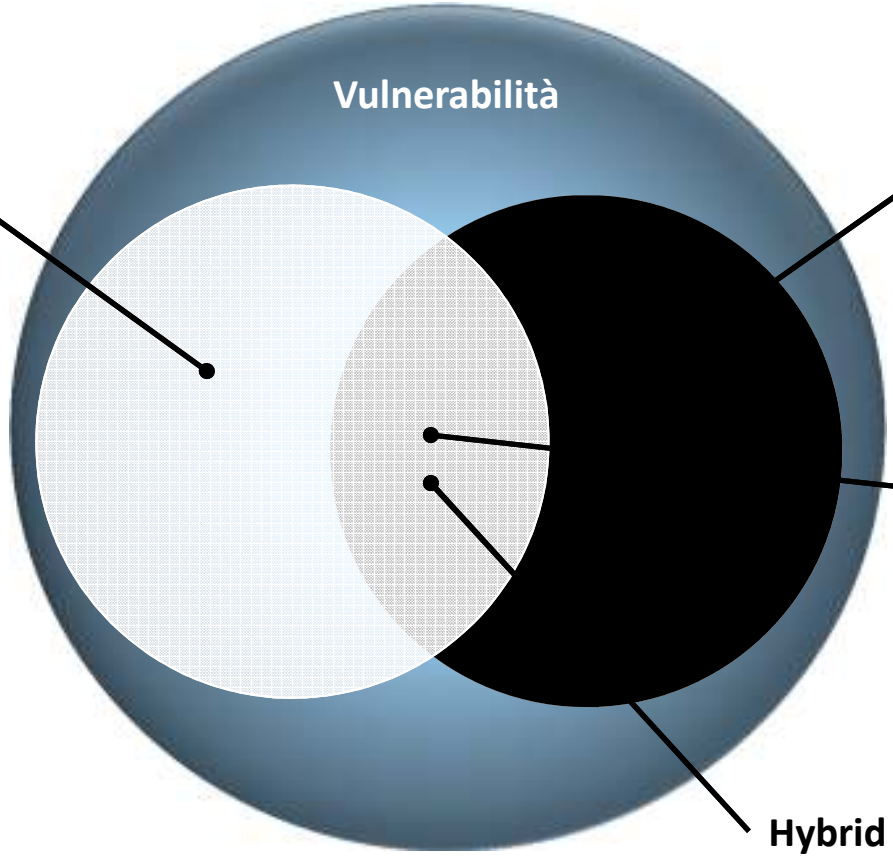
- Oltre agli Use Case, che definiscono gli aspetti funzionali dell'applicazione, è necessario identificare i possibili scenari di attacco o Misuse Cases.



E' importante avere la prospettiva dell'attacker

Rer: http://www.owasp.org/index.php/Testing_Guide_Introduction

Combinazione dei test di sicurezza



Static Analysis

- Null pointer dereference
- Threading issues
- Code quality issues
- Issues in dead code
- Insecure crypto functions
- Issues in back-end application code
- Stored vulnerabilities
- Complex SQL injection

Dynamic Analysis

- Environment configuration issues
- Patch level issues
- Runtime privileges issues
- Authentication issues
- Protocol parser/serializer issues
- Session management issues
- Issues in external 3rd party web components
- Cross-site request forgery
- Malware analysis

Dynamic & Static

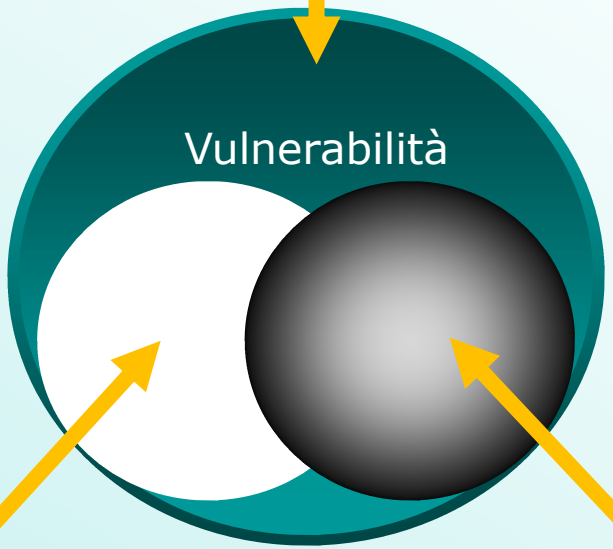
- SQL Injection
- Cross Site Scripting
- HTTP Response Splitting
- OS Commanding
- LDAP Injection
- XPath Injection
- Path Traversal
- Buffer Overflows
- Format String Issues

Hybrid Analysis*

- Client-side issues
  - DOM-based XSS
  - DOM-based Open Redirect
  - HTML5 Notification Phishing
  - HTML5 Client-side SQL Injection
  - Etc.

Non solo i tool…

Architecture review
Code review (manuale)



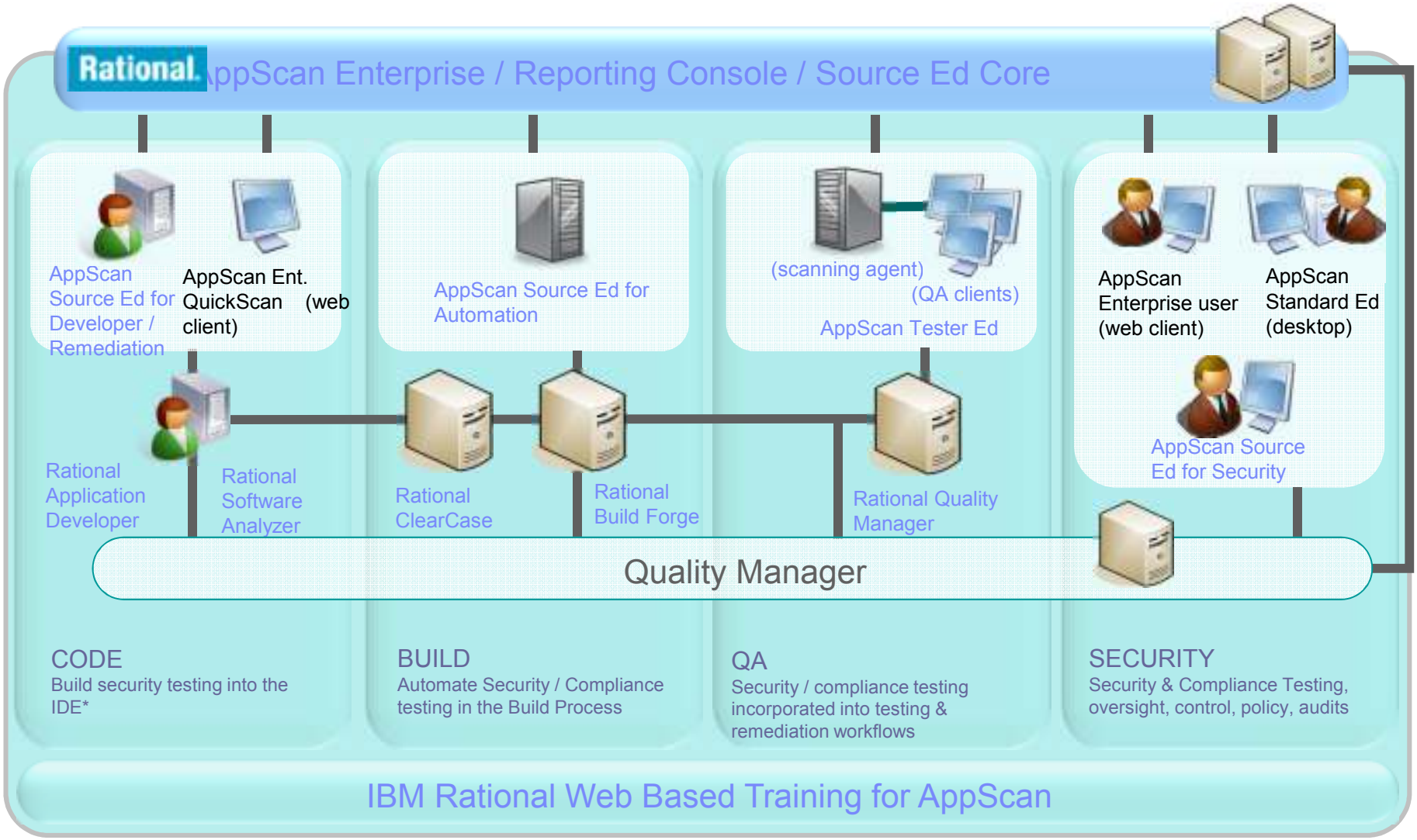
Static Code Analysis (Whitebox)

Dynamic Analysis (Blackbox)

Agenda

- Architetture SCADA
- Secure Engineering
- **IBM Security Solutions**

IBM Rational AppScan Ecosystem



Servizi IBM – Analisi sicurezza sistemi SCADA

Raccolta informazioni	▪ Analisi dell'ambiente ▪ Tipologie di sistemi ▪ Siti da analizzare ▪ Requisiti di sicurezza
Analisi della rete	▪ Approfondimento dell'architettura di rete e dei sistemi ▪ Identificazione dei problemi di sicurezza dell'architettura di rete ▪ Identificazione dei problemi di sicurezza in base all'analisi del traffico ▪ Identificazione delle interconnessione con altre reti - Intranet, wireless, dialup, etc.
Analisi delle vulnerabilità della rete	▪ Analisi vulnerabilità dei dispositivi di rete ▪ Analisi vulnerabilità dei dispositivi delle applicazioni
Analisi delle vulnerabilità dei sistemi	▪ Analisi delle vulnerabilità dei dispositivi ▪ Analisi delle vulnerabilità legate alla configurazione: gestione delle identità, password deboli, etc. ▪ Protezione dai virus, processi e procedure di patch management, system logging etc. ▪ Analisi delle vulnerabilità dei sistemi SCADA ▪ PenTest dei sistemi SCADA
Sicurezza applicativa	▪ **Analisi del processo di sviluppo** ▪ **Definizione del processo di Secure Engineering** ▪ **Definizione delle linee guida per lo sviluppo sicuro** ▪ **Definizione delle metriche e delle metodologie di test**

ICS-ALERT-10-301-01

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) ha emesso un alert riguardo al motore di ricerca SHODAN, che può essere utilizzato per identificare I sistemi SCADA che sono connessi a Internet. Questo può essere sfruttato da parte di attacker per compromettere questi sistemi. ICS-ALERT-10-301-01 descrive una serie di raccomandazioni per ridurre questo rischio.


ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-10-301-01 – CONTROL SYSTEM INTERNET ACCESSIBILITY
October 28, 2010

SUMMARY

The ICS-CERT has recently received several reports from multiple independent security researchers who have employed the SHODAN search engine[1] to discover Internet facing SCADA systems using potentially insecure mechanisms for authentication and authorization. The identified systems span several critical infrastructure sectors and vary in their deployment footprints. ICS-CERT is working with asset owners/operators, Information Sharing and Analysis Centers (ISACS), vendors, and integrators to notify users of these systems about their specific issues; however, due to an increase in reporting of these types of incidents, ICS-CERT is producing a more general alert regarding these issues.

In most cases, the affected control system interfaces were designed to provide remote access for monitoring system status and/or certain asset management features (i.e., configuration adjustments). The identified systems range from stand-alone workstation applications to larger wide area network (WAN) configurations connecting remote facilities to control monitoring systems. These systems have been found to be readily accessible from the Internet and with tools, such as SHODAN, the resources required to identify them has been greatly reduced.

In addition to the increased risk of account brute forcing[2] from having these systems available on the Internet, some of the identify systems continue to use default user names and passwords and/or common vendor accounts[3] for remote access into these systems. These default/common accounts can in many cases be easily found in online documentation and/or online default password repositories. Control System owners and operators are advised to audit their control systems —whether or not directly connected to the Internet— for the use of default administrator level user names and passwords.

Grazie!

Simone Riccetti

Simone.riccetti@it.ibm.com